5437-109

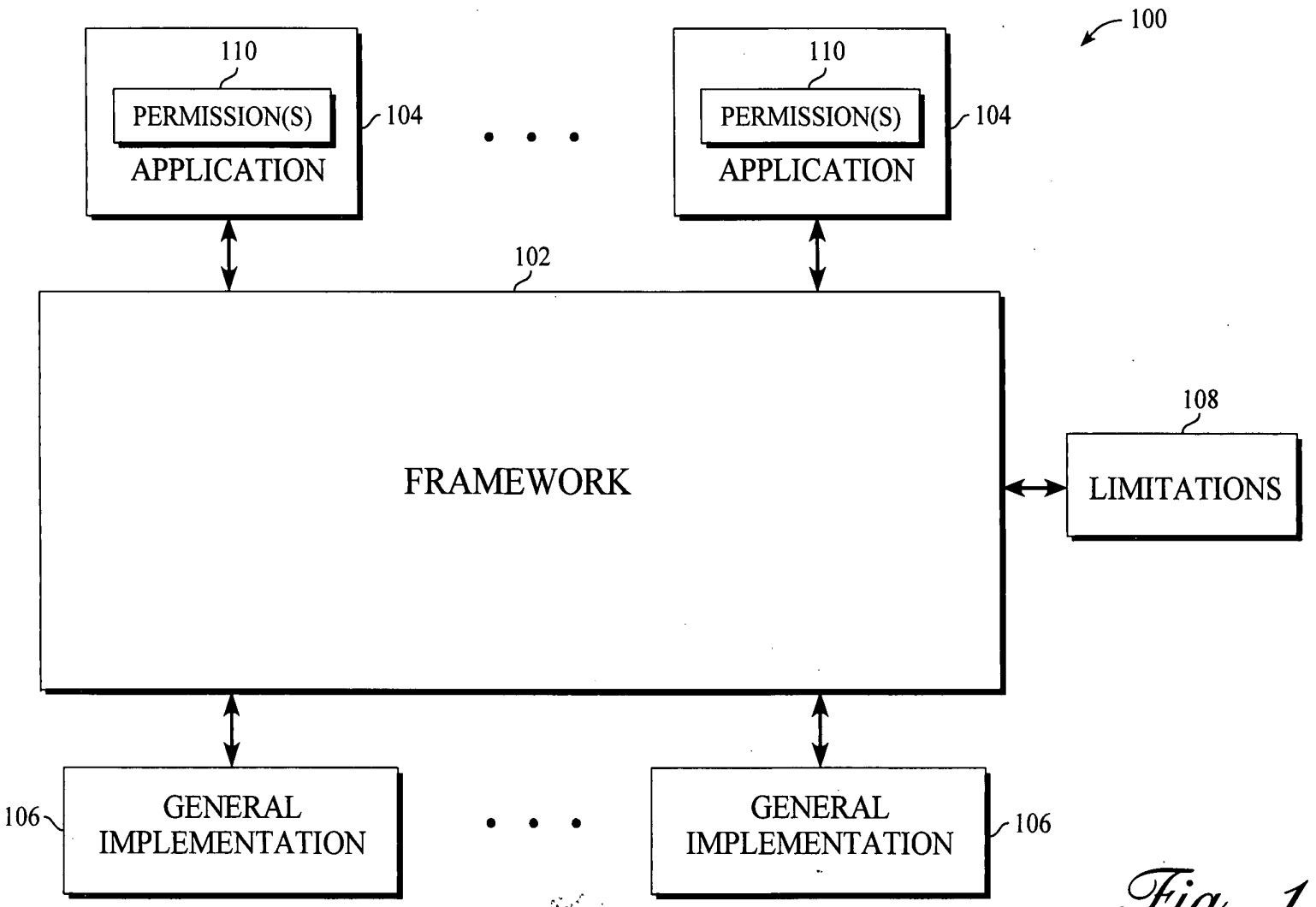

Fig. 1

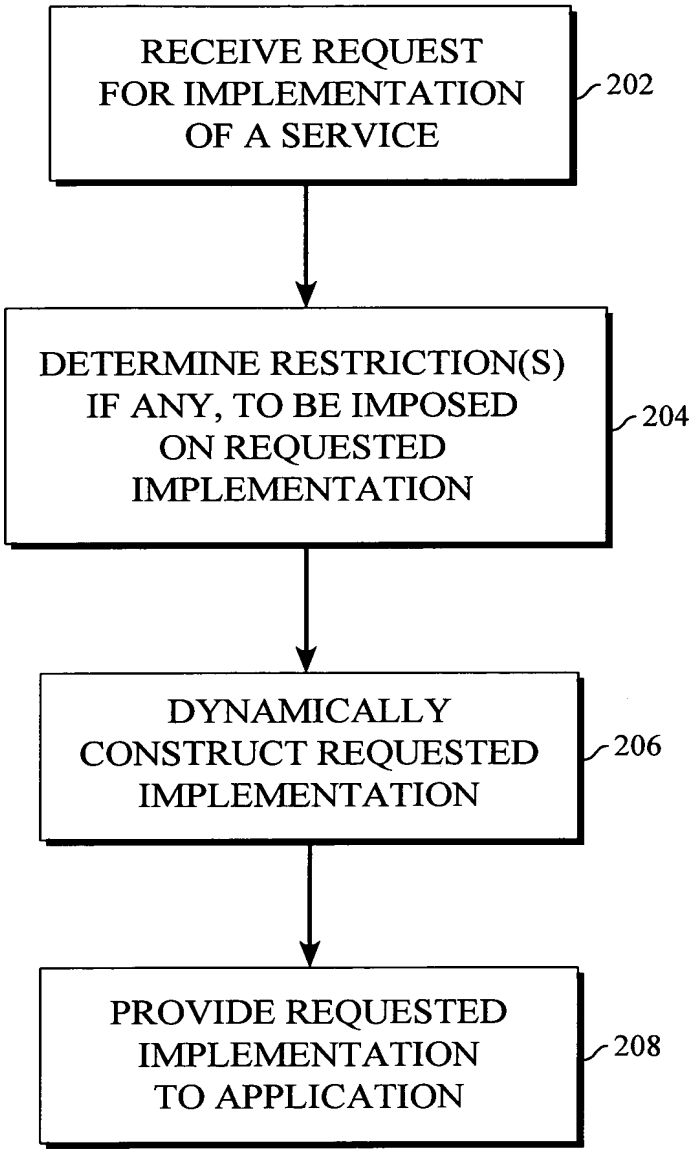

Fig. 2

Docket #: 5437-109

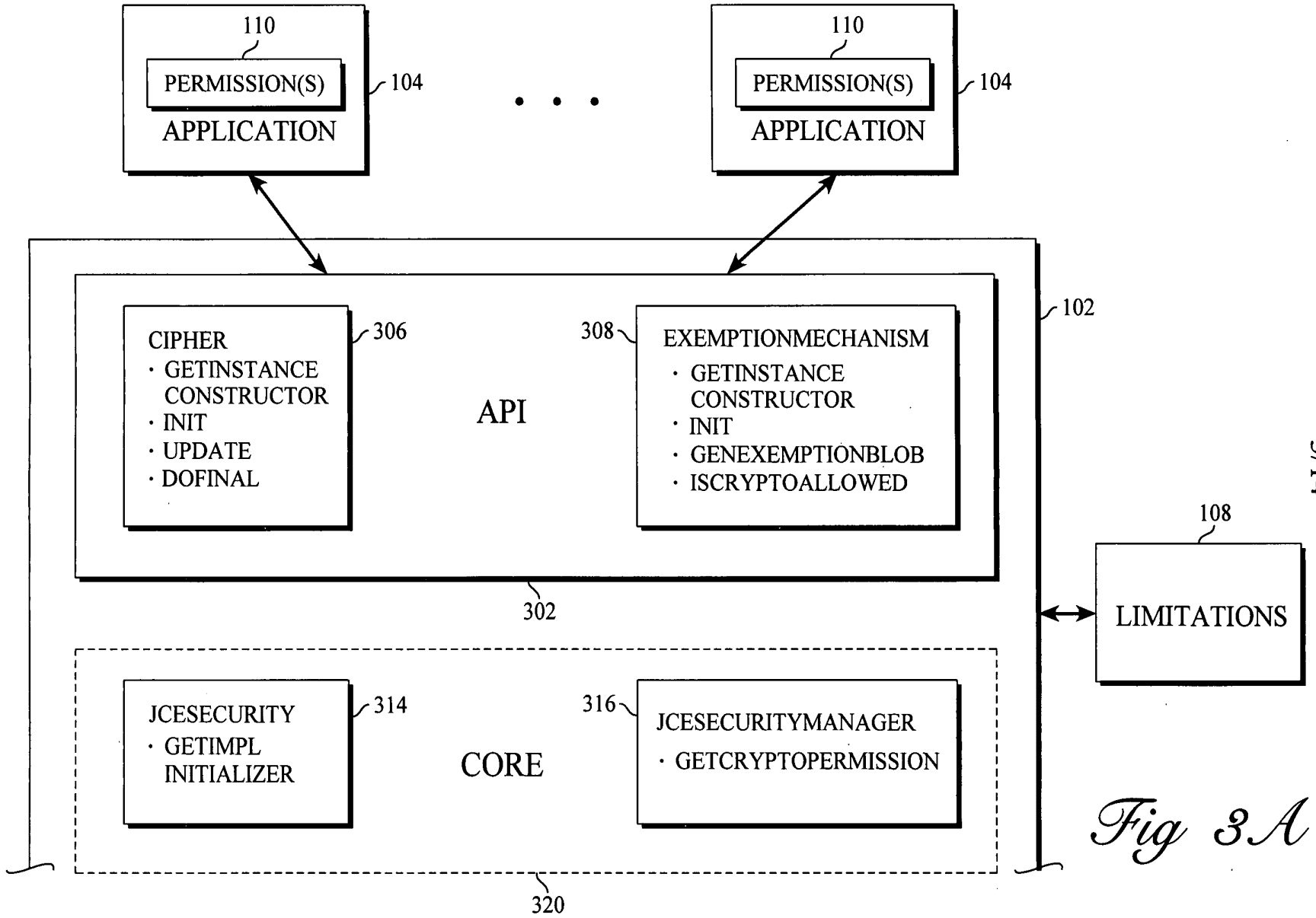
110
PERMISSION(S)
APPLICATION
104
110
PERMISSION(S)
APPLICATION
104
102
CIPHER
· GETINSTANCE CONSTRUCTOR
· INIT
· UPDATE
· DOFINAL
306
API
308
EXEMPTIONMECHANISM
· GETINSTANCE CONSTRUCTOR
· INIT
· GENEXEMPTIONBLOB
· ISCRYPTOALLOWED
302
108
LIMITATIONS
JCESECURITY
· GETIMPL INITIALIZER
314
CORE
316
JCESECURITYMANAGER
· GETCRYPTOPERMISSION
320

Fig 3A

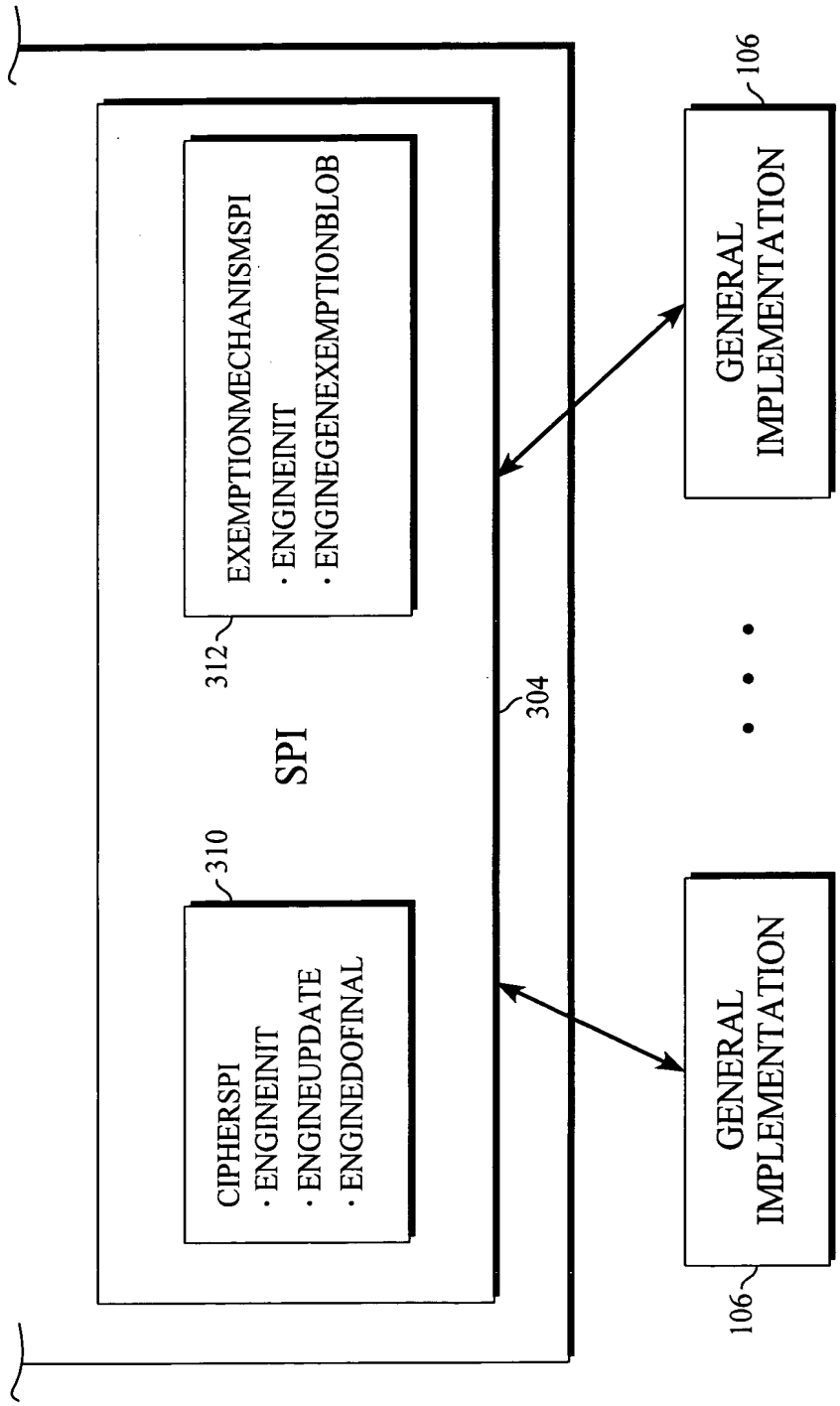
CIPHERSPI
· ENGINEINIT
· ENGINEUPDATE
· ENGINEDOFINAL
310
SPI
312
EXEMPTIONMECHANISMSPI
· ENGINEINIT
· ENGINEGENEXEMPTIONBLOB
304
GENERAL IMPLEMENTATION
106
GENERAL IMPLEMENTATION
106

Fig. 3B

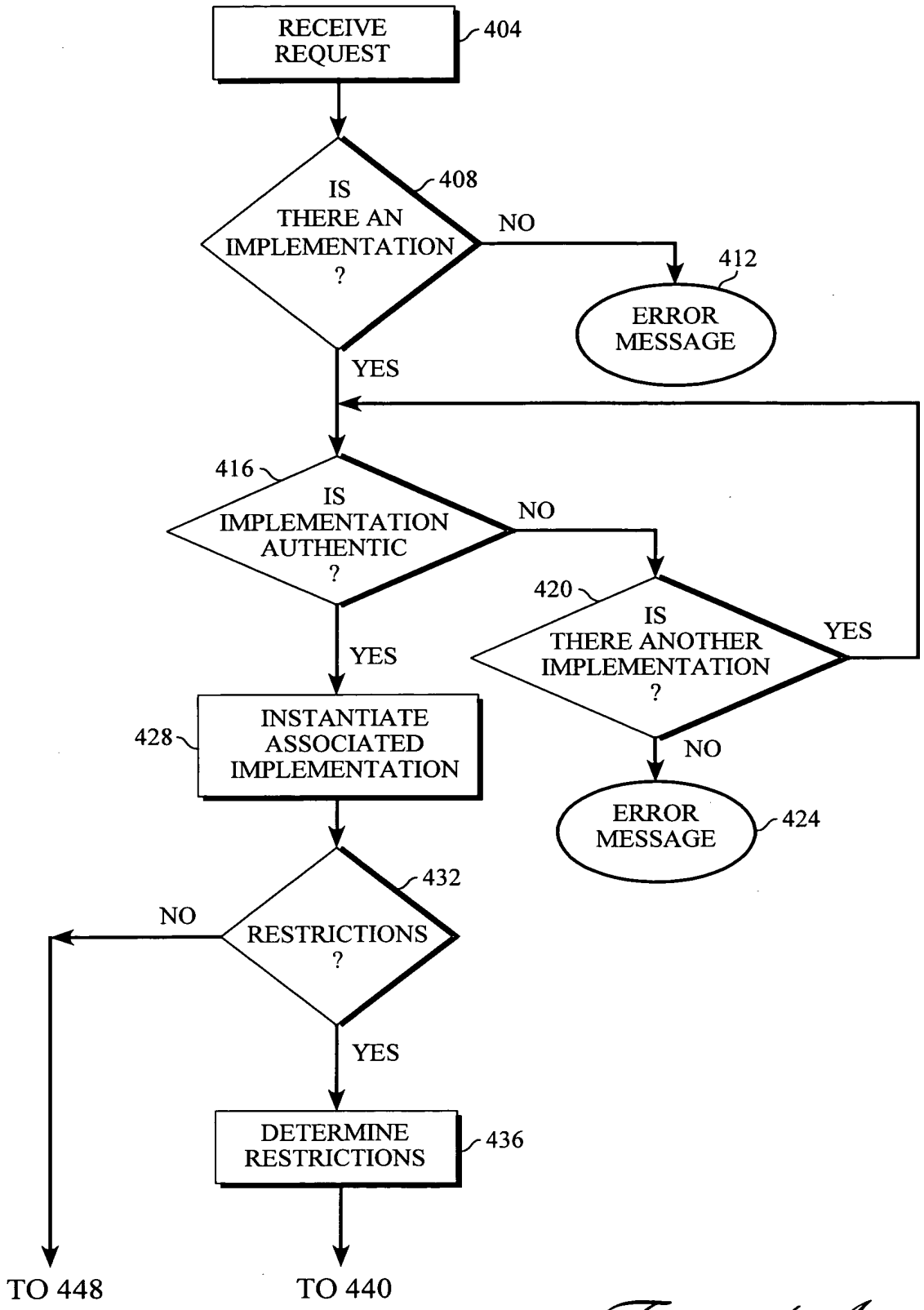

Fig. 4A

Docket No. 5437-109

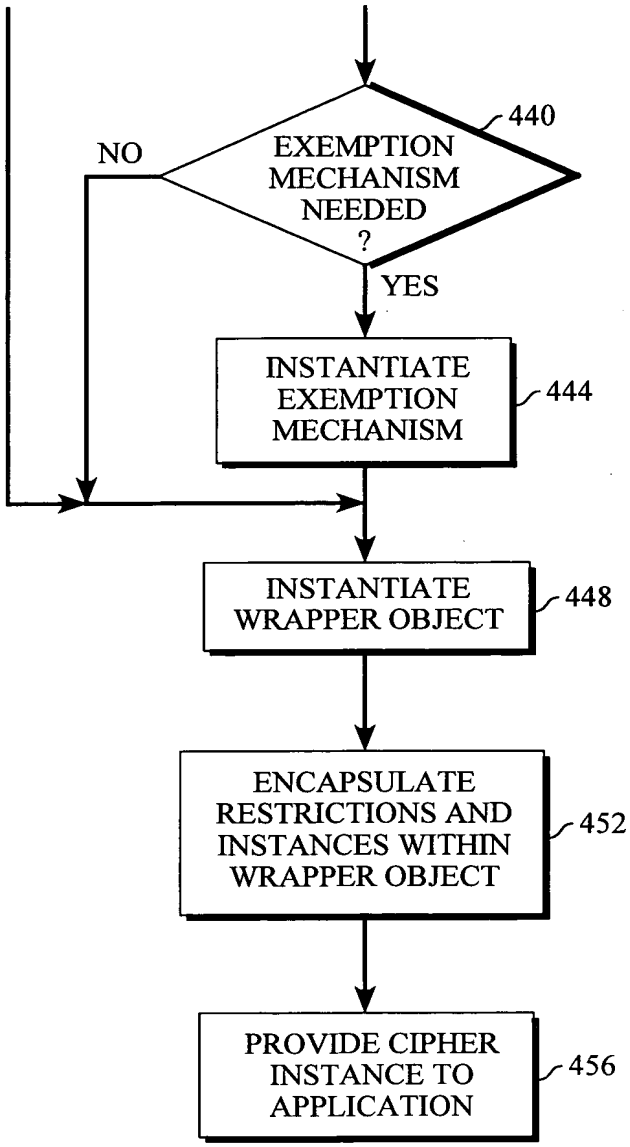
EXEMPTION MECHANISM NEEDED ?
440
NO
YES
INSTANTIATE EXEMPTION MECHANISM
444
INSTANTIATE WRAPPER OBJECT
448
ENCAPSULATE RESTRICTIONS AND INSTANCES WITHIN WRAPPER OBJECT
452
PROVIDE CIPHER INSTANCE TO APPLICATION
456

Fig. 4B

DEFAULT SET

(1) ALGORITHM NAME: BLOWFISH

EXEMPTION MECHANISM :
MAX KEY SIZE : 128 BITS
OTHER LIMITATION (S) :

(2) ALGORITHM NAME: DES

EXEMPTION MECHANISM :
MAX KEY SIZE : 128 BITS
OTHER LIMITATION (S) :

(3) ALGORITHM NAME: RC5

EXEMPTION MECHANISM :
MAX KEY SIZE : 64 BITS
OTHER LIMITATION (S) : 10 ROUNDS

EXEMPT SET

(1) ALGORITHM NAME: BLOWFISH

EXEMPTION MECHANISM : KEY RECOVERY
MAX KEY SIZE : 256 BITS
OTHER LIMITATION (S) :

(2) ALGORITHM NAME: BLOWFISH

EXEMPTION MECHANISM : KEY ESCROW
MAX KEY SIZE : 256 BITS
OTHER LIMITATION (S) :

Fig. 5

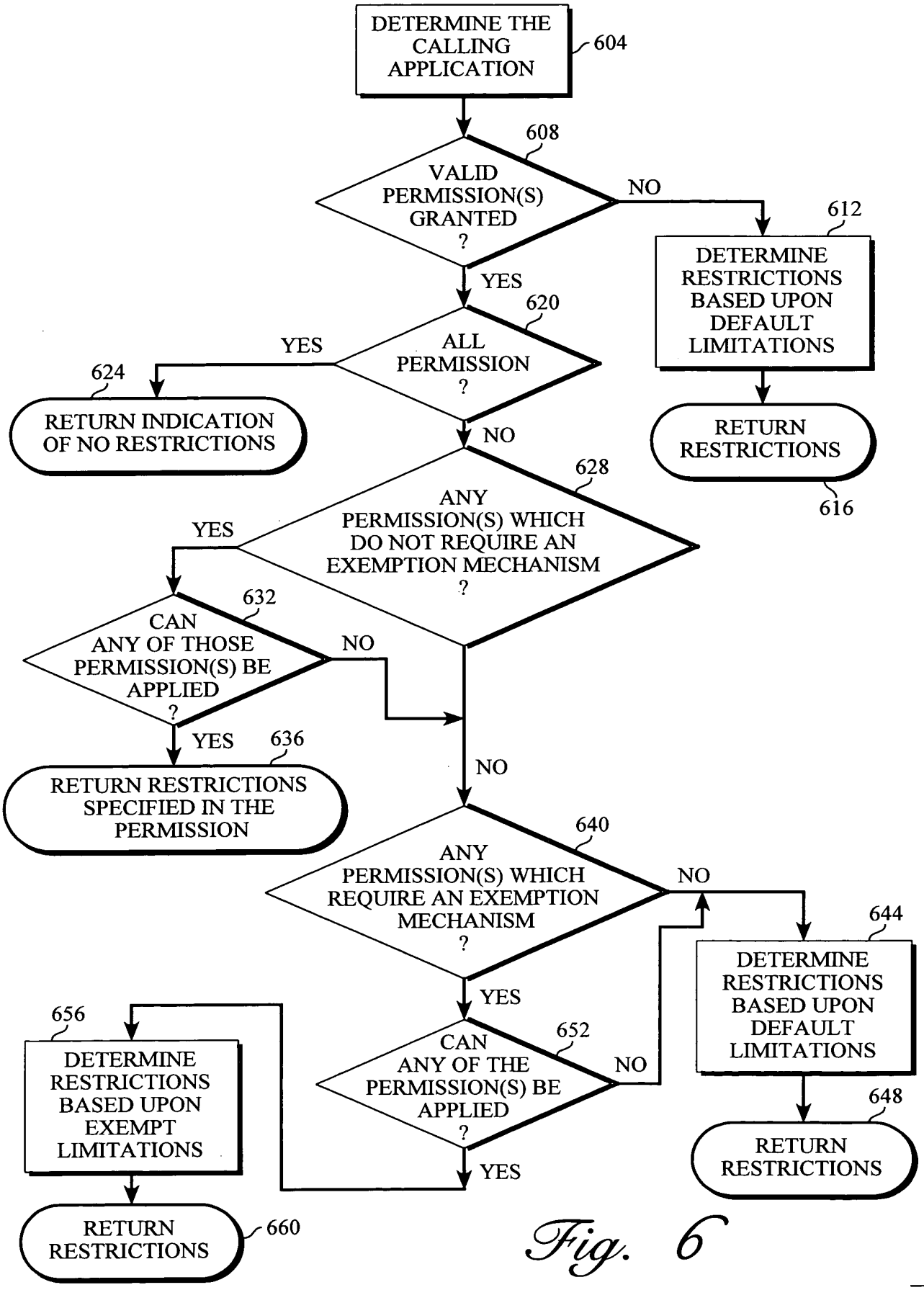
DETERMINE THE CALLING APPLICATION
604
608
VALID PERMISSION(S) GRANTED ?
NO
612
DETERMINE RESTRICTIONS BASED UPON DEFAULT LIMITATIONS
YES
620
ALL PERMISSION ?
YES
624
RETURN INDICATION OF NO RESTRICTIONS
NO
628
ANY PERMISSION(S) WHICH DO NOT REQUIRE AN EXEMPTION MECHANISM ?
RETURN RESTRICTIONS
616
YES
632
CAN ANY OF THOSE PERMISSION(S) BE APPLIED ?
NO
YES
636
RETURN RESTRICTIONS SPECIFIED IN THE PERMISSION
NO
640
ANY PERMISSION(S) WHICH REQUIRE AN EXEMPTION MECHANISM ?
NO
644
DETERMINE RESTRICTIONS BASED UPON DEFAULT LIMITATIONS
YES
656
652
CAN ANY OF THE PERMISSION(S) BE APPLIED ?
NO
DETERMINE RESTRICTIONS BASED UPON EXEMPT LIMITATIONS
YES
648
RETURN RESTRICTIONS
RETURN RESTRICTIONS
660

Fig. 6

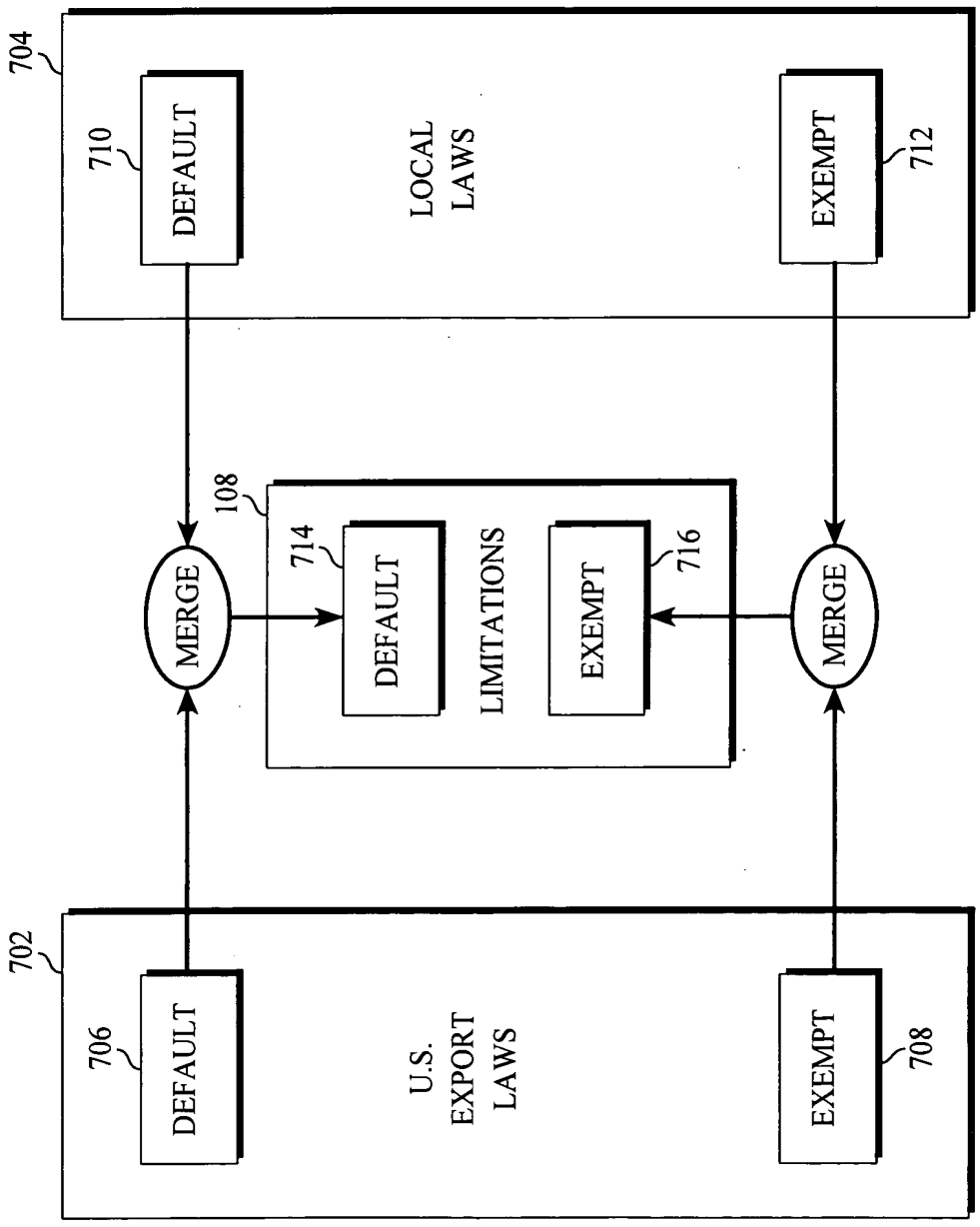
704
710
DEFAULT
LOCAL
LAWS
712
EXEMPT
108
714
DEFAULT
LIMITATIONS
EXEMPT
716
MERGE
MERGE
702
706
DEFAULT
U.S.
EXPORT
LAWS
EXEMPT
708

Fig. 7

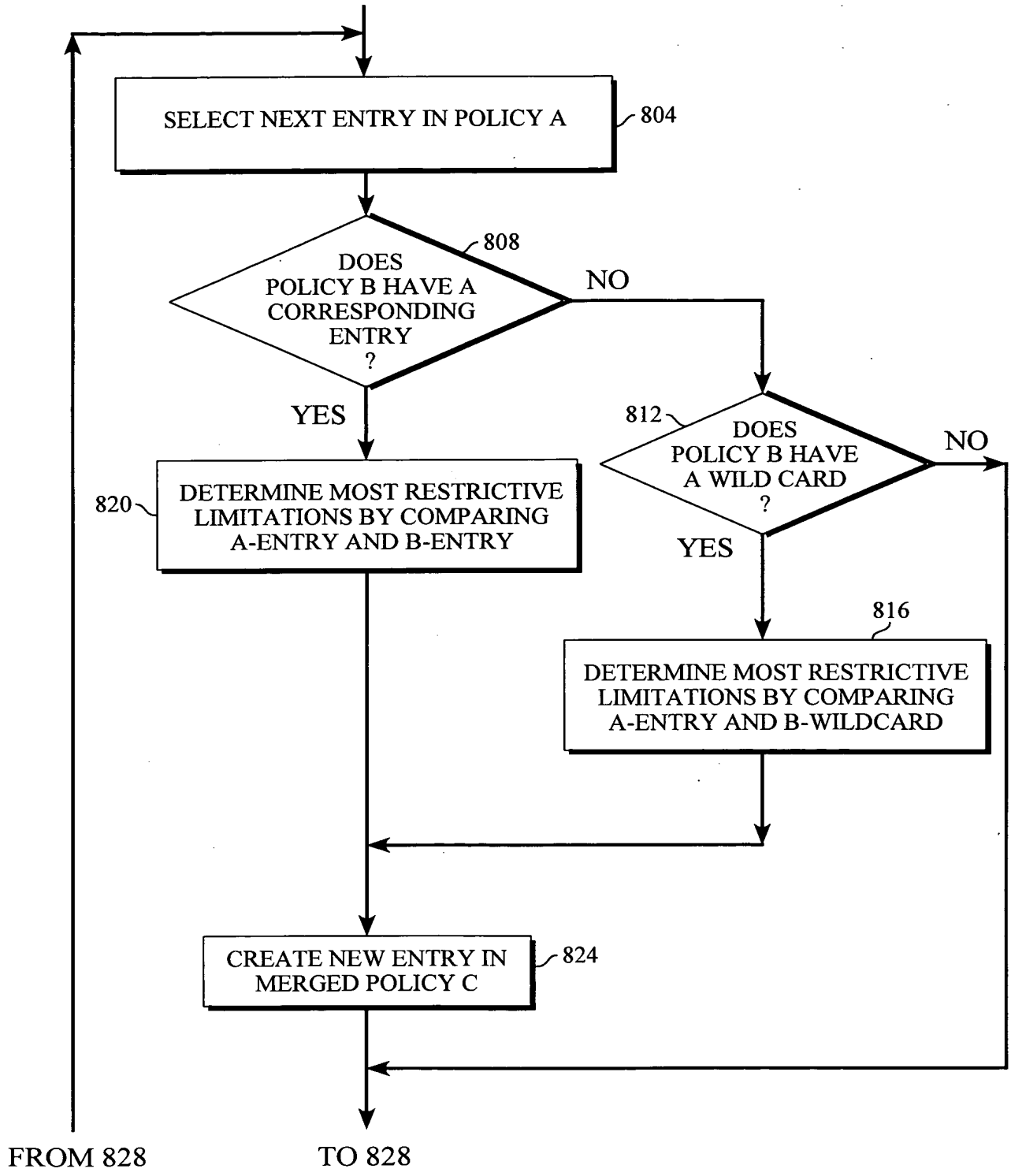
SELECT NEXT ENTRY IN POLICY A
804
DOES POLICY B HAVE A CORRESPONDING ENTRY ?
808
NO
YES
DETERMINE MOST RESTRICTIVE LIMITATIONS BY COMPARING A-ENTRY AND B-ENTRY
820
812
DOES POLICY B HAVE A WILD CARD ?
NO
YES
816
DETERMINE MOST RESTRICTIVE LIMITATIONS BY COMPARING A-ENTRY AND B-WILDCARD
CREATE NEW ENTRY IN MERGED POLICY C
824
FROM 828
TO 828

Fig. 8A

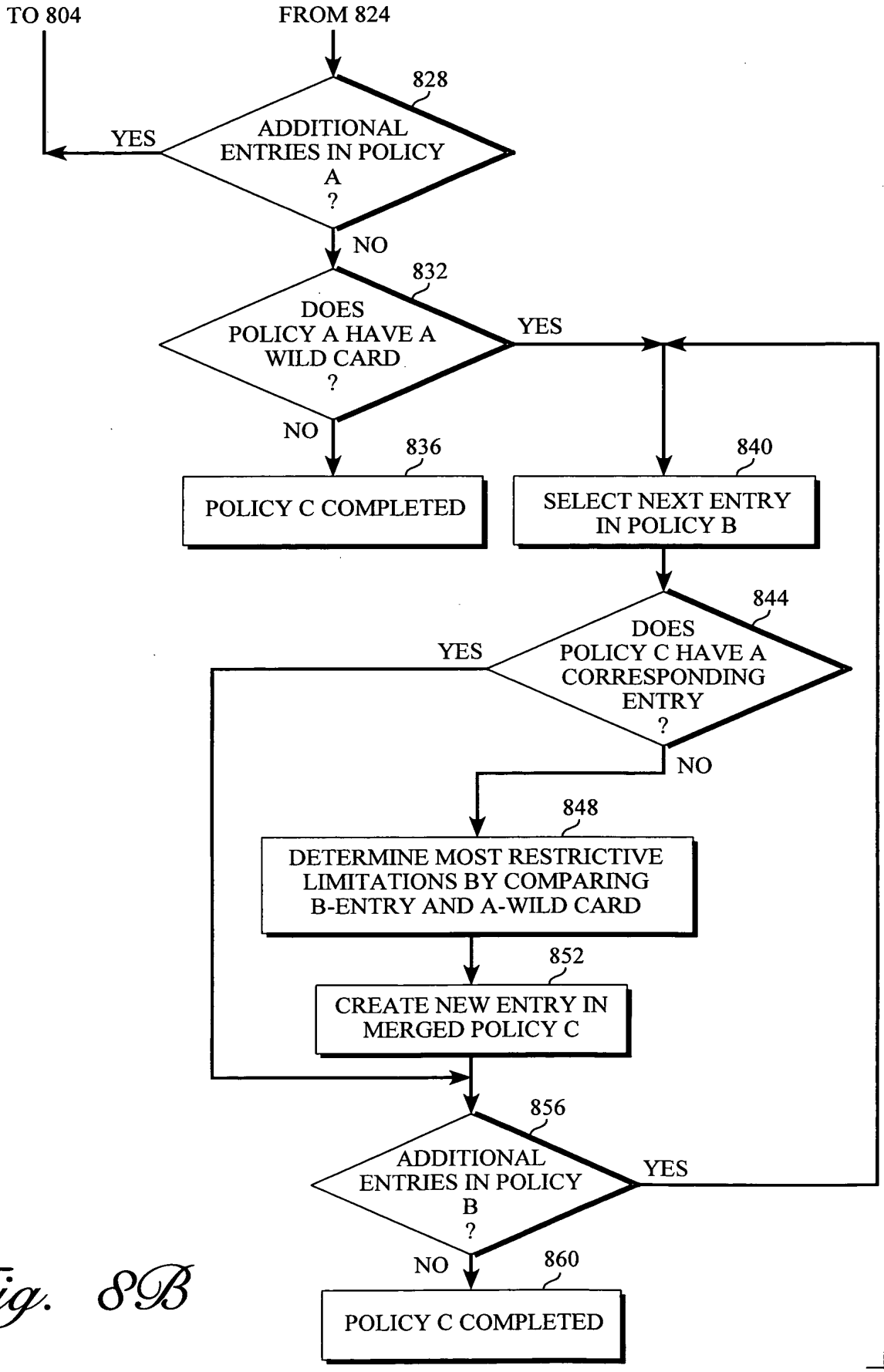
TO 804
FROM 824
828
ADDITIONAL ENTRIES IN POLICY A ?
YES
NO
832
DOES POLICY A HAVE A WILD CARD ?
YES
NO
836
POLICY C COMPLETED
840
SELECT NEXT ENTRY IN POLICY B
844
DOES POLICY C HAVE A CORRESPONDING ENTRY ?
YES
NO
848
DETERMINE MOST RESTRICTIVE LIMITATIONS BY COMPARING B-ENTRY AND A-WILD CARD
852
CREATE NEW ENTRY IN MERGED POLICY C
856
ADDITIONAL ENTRIES IN POLICY B ?
YES
NO
860
POLICY C COMPLETED

Fig. 8B

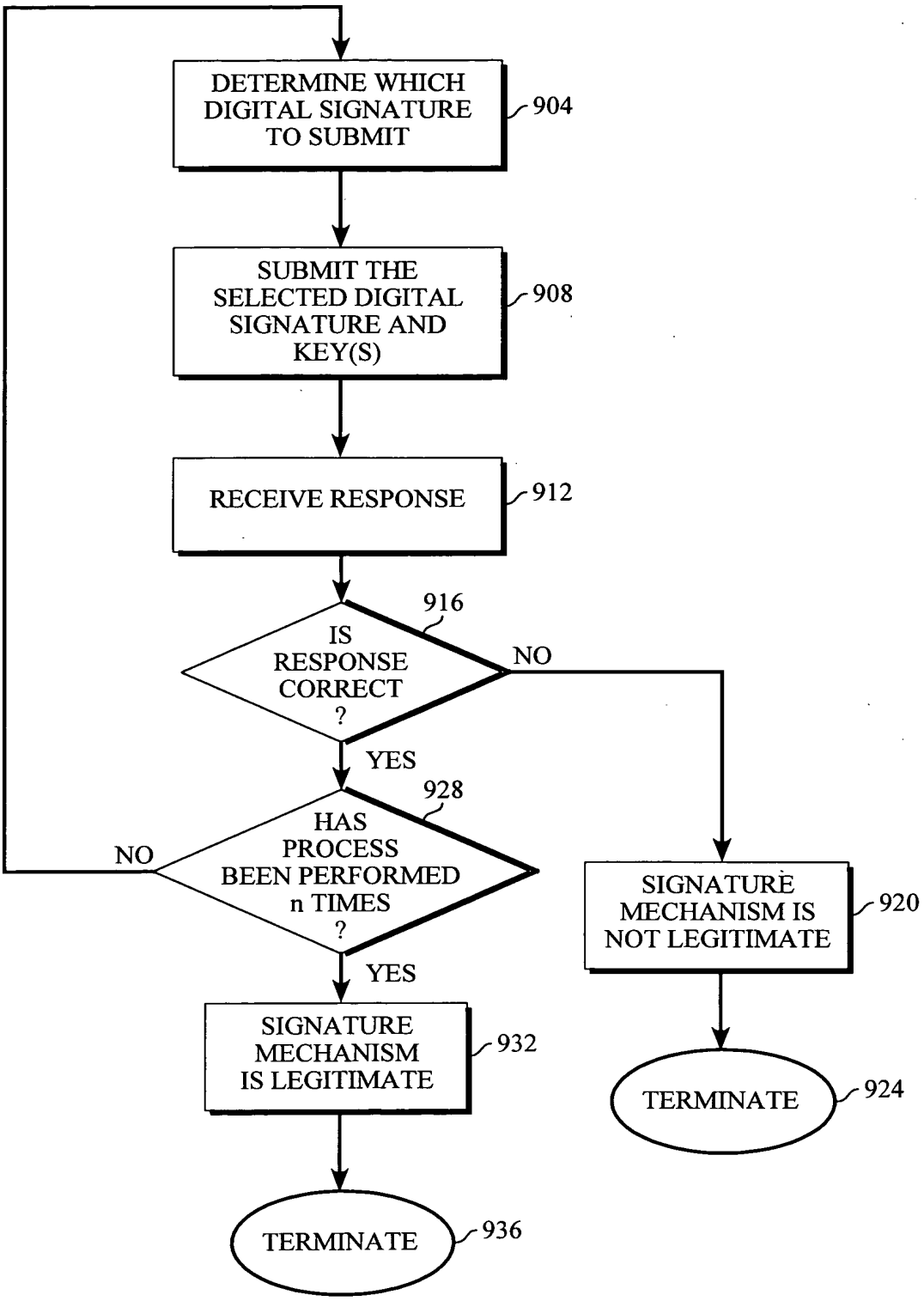
DETERMINE WHICH DIGITAL SIGNATURE TO SUBMIT
904
SUBMIT THE SELECTED DIGITAL SIGNATURE AND KEY(S)
908
RECEIVE RESPONSE
912
916
IS RESPONSE CORRECT ?
NO
YES
928
HAS PROCESS BEEN PERFORMED n TIMES ?
NO
YES
SIGNATURE MECHANISM IS NOT LEGITIMATE
920
TERMINATE
924
SIGNATURE MECHANISM IS LEGITIMATE
932
TERMINATE
936

Fig. 9

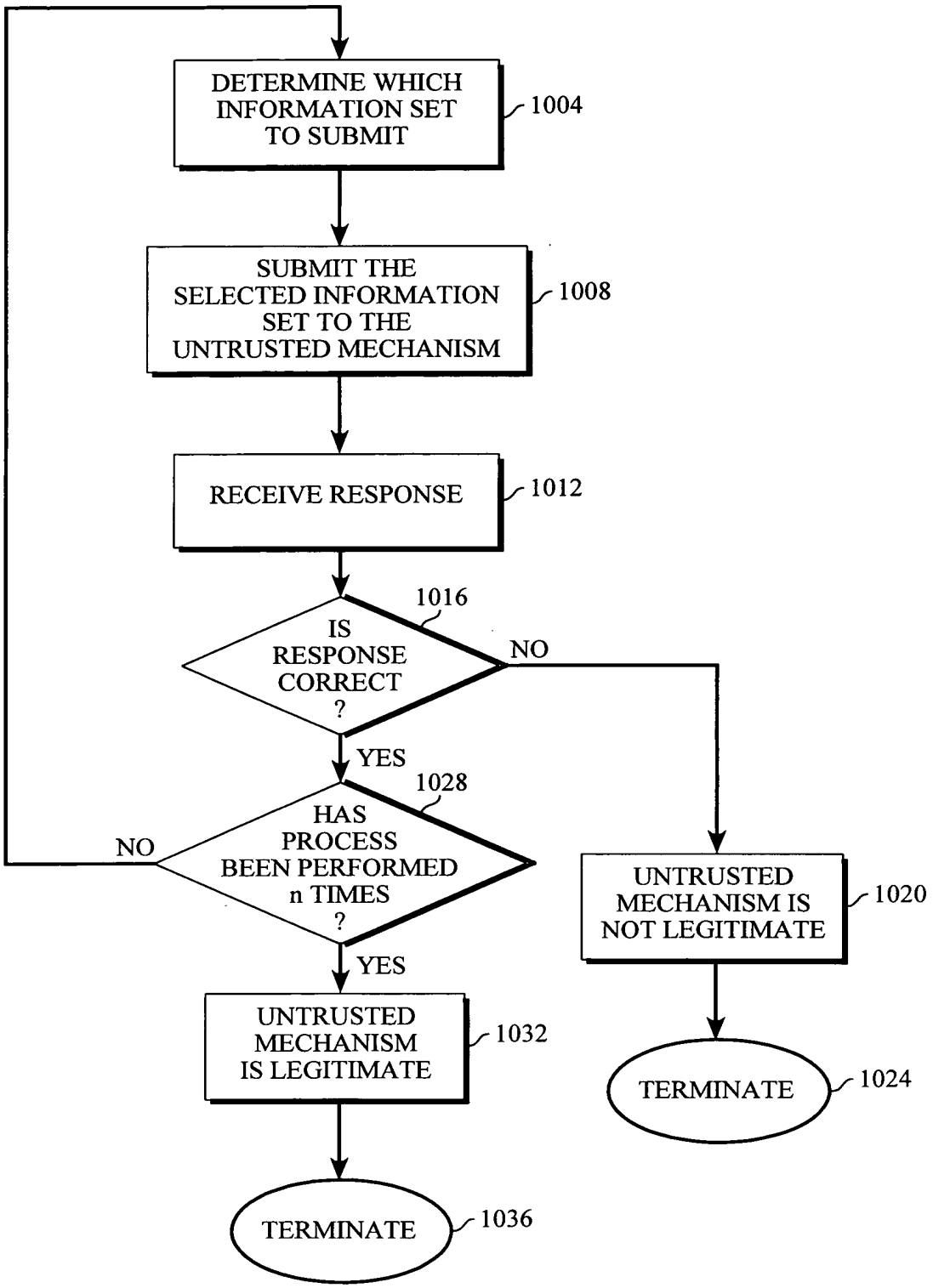
DETERMINE WHICH INFORMATION SET TO SUBMIT
1004
SUBMIT THE SELECTED INFORMATION SET TO THE UNTRUSTED MECHANISM
1008
RECEIVE RESPONSE
1012
1016
IS RESPONSE CORRECT ?
NO
YES
1028
HAS PROCESS BEEN PERFORMED n TIMES ?
NO
YES
UNTRUSTED MECHANISM IS NOT LEGITIMATE
1020
UNTRUSTED MECHANISM IS LEGITIMATE
1032
TERMINATE
1024
TERMINATE
1036

Fig. 10

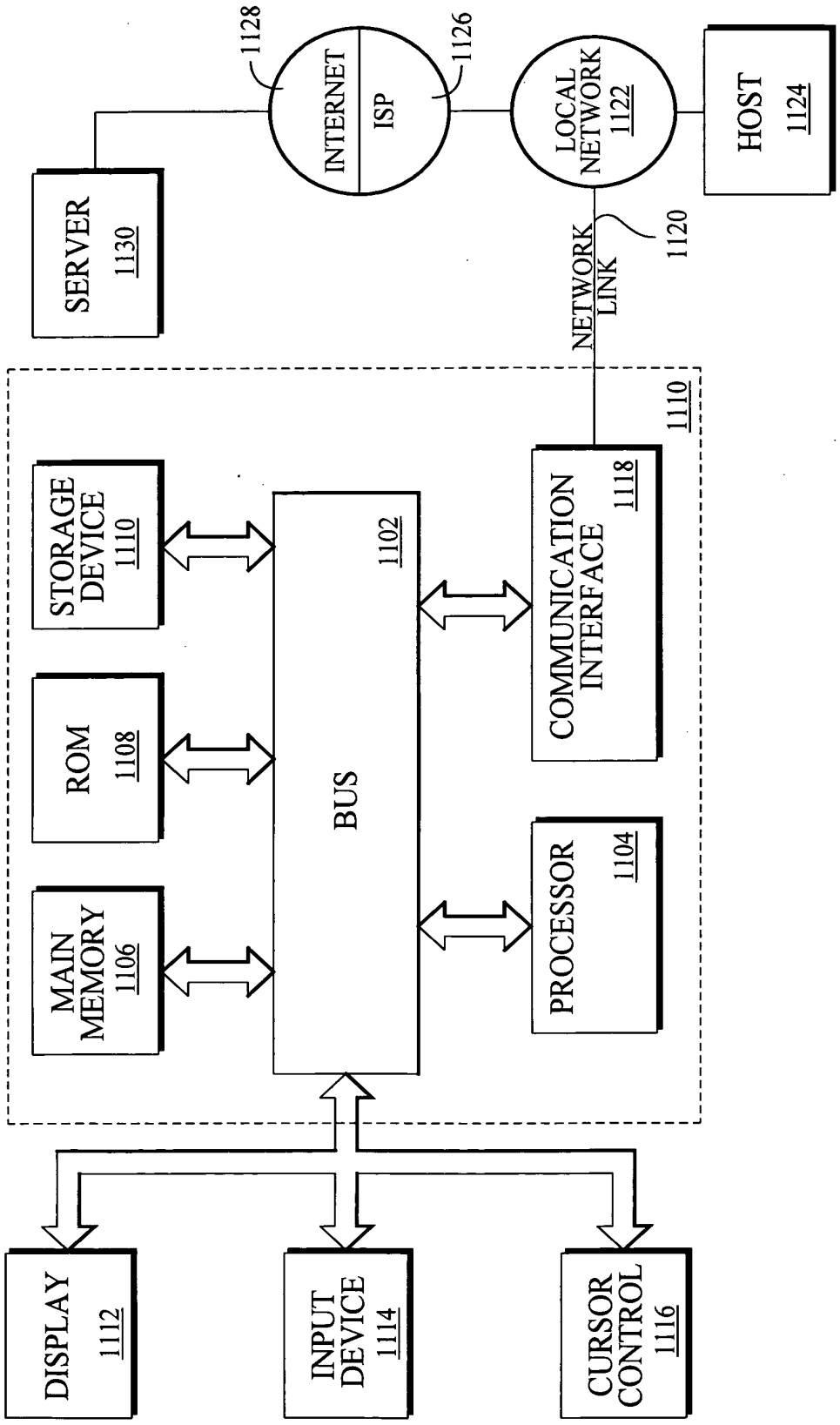
SERVER
1130
1128
INTERNET
ISP
1126
LOCAL NETWORK
1122
HOST
1124
NETWORK LINK
1120
1110
STORAGE DEVICE
1110
ROM
1108
MAIN MEMORY
1106
BUS
1102
COMMUNICATION INTERFACE
1118
PROCESSOR
1104
DISPLAY
1112
INPUT DEVICE
1114
CURSOR CONTROL
1116

Fig. 11